特許請求の範囲

1．可変認証情報を用いる資格認証方法であって、初期登録フェーズおよび認証フェーズを有し、

前記初期登録フェーズは、

被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、入力情報を算出することが計算量的に困難であるような一方向性を有する出力情報を生成する一方向性関数を用いて初回の認証データを生成する工程と、

被認証者が認証者に対して、自己のユーザーＩＤと初回の認証データを送信する工程と、

認証者が被認証者から受信した初回の認証データを初回認証時に用いる認証パラメータとして登録する工程を有し、

前記認証フェーズは、被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、前記一方向性関数を用いて今回の認証データ用中間データと今回の認証データと次回の認証データと認証確認用中間パラメータを生成し、今回の認証データ用中間データに今回の認証データと認証確認用中間パラメータで排他的論理和演算を行うと共に，次回の認証データに今回の認証データで排他的論理和演算することにより、今回認証用の排他的論理和及び次回認証用の排他的論理和を生成する工程と、

被認証者が認証者に対して、自己のユーザーＩＤ、今回認証用の排他的論理和及び次回認証用の排他的論理和を送信する工程と、

認証者が、被認証者から受信した次回認証用の排他的論理和と前回登録された認証パラメータとの排他的論理和により次回認証用仮パラメータを生成し、次回認証用仮パラメータから前記一方向性関数を用いて認証確認用中間パラメータを生成する工程と，

被認証者から受信した今回認証用の排他的論理和と前回登録された認証パラメータと生成された認証確認用中間パラメータとの排他的論理和を入力情報として、前記一方向性関数を用いて被認証者の正当性確認パラメータを生成し、この正当性確認パラメータと前回登録された認証パラメータを比較し、一致した場合は認

証が成立したものとし、一致しない場合は認証が不成立と判断する工程と、

認証が成立した場合は、前回登録された認証パラメータの替わりに前記の次回認証用仮パラメータを次回認証用の認証パラメータとして登録する工程を有する。

２．請求項１記載の方法であって、前記一方向性関数Ｅとして、秘密鍵暗号方式に用いる関数を用いる。

３．請求項１記載の方法であって、一方向性関数Ｅとして、ＤＥＳまたはＦＥＡＬ関数を用いる。